UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,291	04/16/2004	Catherine Helen Gebotys	1679-14/EDEV	7948

38735 7590 11/25/2008

DIMOCK STRATTON LLP
20 QUEEN STREET WEST SUITE 3202, BOX 102
TORONTO, ON M5H 3R3
CANADA

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
11/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/825,291	GEBOTYS, CATHERINE HELEN	
	Examiner	Art Unit	
	Thanhnga B. Truong	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) *1-8,14-29 and 35-58* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-13 and 30-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on August 29, 2008. Claims 1-58 are pending. Claims 1-8, 14-29, and 35-58 are cancelled by the applicant. At this time, claims 9-13 and 30-34 are rejected.

Election/Restrictions

2. Applicant's election with traverse of **Species 2** in the reply filed on August 29, 2008 is acknowledged.

Claims 1-8, 14-29, and 35-58 are withdrawn and cancelled by the applicant from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected species 1 and species 3. Election was made with traverse in the reply filed on August 29, 2008. This is not found persuasive because each of the various disclosed species details a mutual exclusive characteristic of:

Species 1 is drawn to "A computing device-implemented method, program product, and/or system for carrying out encryption using a key value for encrypting a plaintext value to define a cipher text, the encryption being defined using an encryption function."

Species 2 is drawn to "A countermeasure method, program product, and/or system for resisting security attacks on a processing unit using a key to perform a defined cryptographic function and/or to encrypt a plaintext value using a look up on a table."

Species 3 is drawn to "A computing device-implemented method, program product, and/or system for use with an AES key generation process for defining masked round keys for use in AES encryption."

These above individual species act as evidenced by the representation of each various species with a different figure or set of figures.

A search for one of these mutually exclusive characteristics is not coextensive with a search for the other mutually exclusive characteristics and therefore searching for all mutually exclusive characteristics could not be done without serious burden. The requirement is still deemed proper and is therefore made FINAL.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States..

4. Claims 9-13 and 30-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Kocher et al (US 6,278,783 B1).

a. *Referring to claim 9:*

i. Kocher teaches a countermeasure method for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the method comprising the following steps:

(1) obtaining the key and a random value r **(see Figure 1, element 100; column 8, line 65 through column 9, line 13 of Kocher)**;

(2) obtaining a set of n random input values m.sub.in1, ...m.sub.inn **(column 6, lines 39-45 of Kocher);**

(3) defining a masked function by masking the defined cryptographic function with the value m.sub.in1^...^m.sub.inn **(see Figure 2, element 220; column 8, lines 31-51 of Kocher);**

(4) masking the key with the random value r to define the value mkey **(see Figure 2, element 220; column 7, lines 30-33; column 8, lines 31-51 of Kocher);**

(5) obtaining a set of random values m1, . . . mn-1 **(column 6, lines 40-55; column 7, lines 30-48 of Kocher);**

(6) defining a value mn to be r^m.sub.in1^...^m.sub.inn^m1^ . . . ^mn-1 **(see Figure 2; column 7, lines 30-33; column 8, lines 31-51 of Kocher);** and

(7) using the values m1, . . . , mn and mkey to define input for the masked function **(see Figure 2, element 220; column 8, lines 31-51 of Kocher);**

b. *Referring to claim 10:*

i. Kocher further teaches:

(1) in which the encryption function is a table look-up **(column 5, lines 7-32 of Kocher).**

c. *Referring to claim 11:*

i. Kocher further teaches:

(1) in which masking is a bitwise exclusive or operation carried out on binary values **(column 2, lines 25-29 of Kocher).**

d. *Referring to claims 12-13:*

i. These claims have limitations that is similar to those of claims 9-11, thus they are rejected with the same rationale applied against claims 9-11 above.

e. *Referring to claims 30-32:*

i. This claim consists a computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium to implement claims 9-11 and thus they are rejected with the same rationale applied against claims 9-11 above.

f. *Referring to claims 33-34:*

i. This claim consists a computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said

medium to implement claims 9-11 and thus they are rejected with the same rationale applied against claims 9-11 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Johnson et al (US 6,052,469) discloses Interoperable Cryptographic Key Recovery System with Verification by Comparison (see Title).

b. Ito et al (US 7,386,130 B2) discloses Encryption Secured Against DPA (see Title).

c. Liardet et al (US 7,403,620 B2) discloses Cyphering/Decyphering Performed by an Integrated Circuit (see Title).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2435

TBT
November 26, 2008